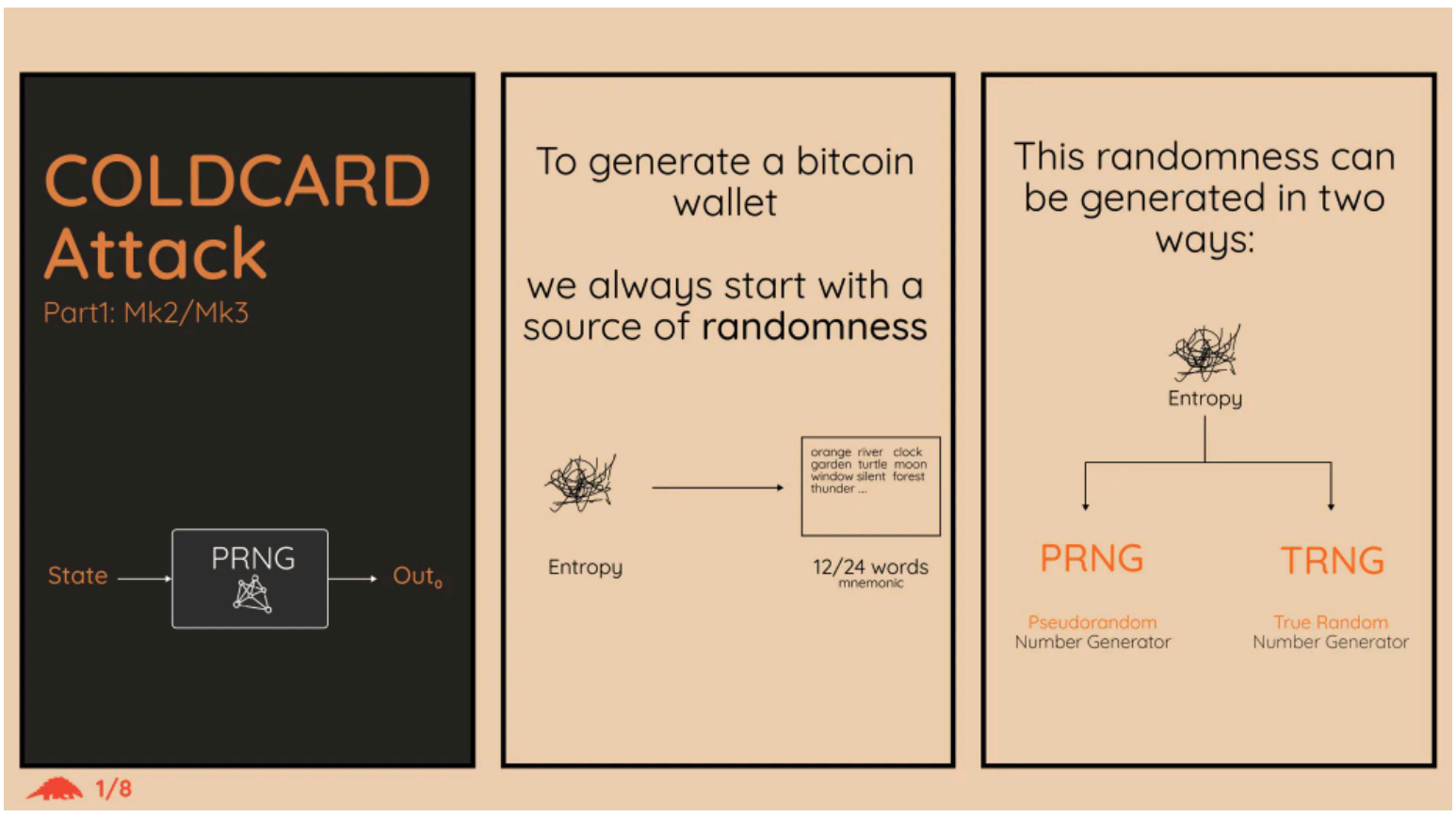
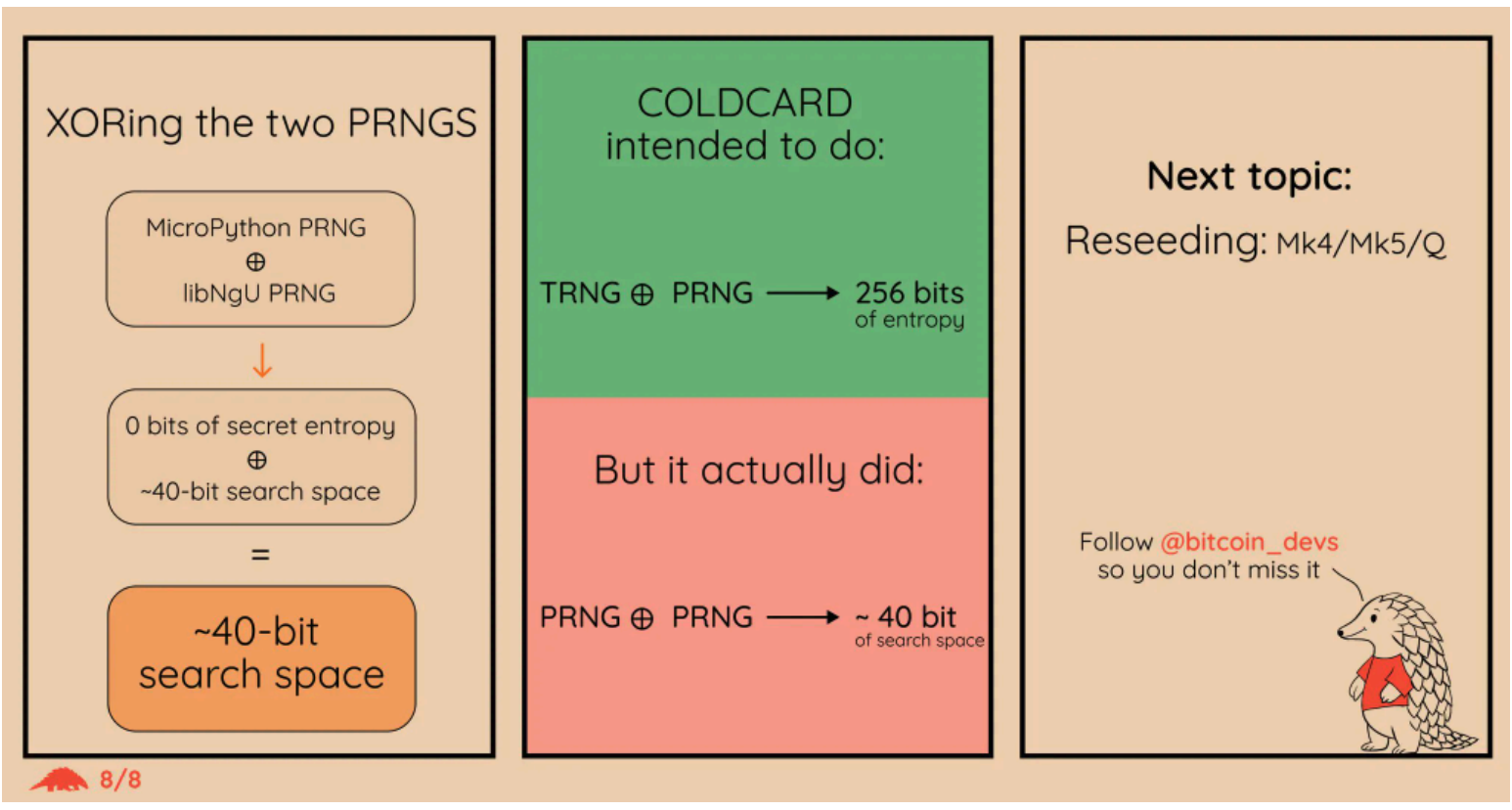
LISTEDRESERVE
MoneyBits

Where to turn?

On Friday last week, news began to filter through of a weakness in a bitcoin wallet known as ColdCard. It's a rather niche product from a small company but nonetheless well known amongst bitcoiners, predominantly because of their highly vocal CEO who goes by the moniker @nvk. Naturally, the website explaining the whole debacle is called [nvk.wtf](nvk.wtf). I present only the first and last slide here.





In essence, the firmware on affected ColdCard devices was not properly using randomness to generate seed words, for no other reason than the code did not ask it to (although they believed it had). As a result, a hacker is now quietly making their way through various possibilities for seed words on ColdCard devices, essentially because those seed words are now deterministic, not random. With enough guesses a computer can get to the seed word and recreate the wallet.

Emerging with tremendous credit from all of this was Jack Dorsey's Block. Their post on the specifics of the issue was excellent. It pretty much lays bare that this is a straight up coding error that exposed ColdCard users to a vulnerability. It also revealed that some American companies have access to AI tools that others do not.

There is a more interesting point here though. The vulnerability was allegedly found by LLM Kimi K3, it has existed for over five years so its discovery correlates closely with the new abilities of the open-source models. To test the hypothesis (feel free to do the same), I gave the details of the Block post, which specifically highlights the weakness, to ChatGPT 5.6 and Claude Fable. Instantly, both refused to participate in any sort of analysis because the findings 'could be used to exploit the weakness'. True. I then used a combination of Chinese models GLM and then Kimi itself (which gave one refusal before helping). They not only diagnosed the specifics of the vulnerability but described how one could look for it elsewhere, with a view to preventing it, and let's be honest you could entirely use that to exploit it as well. Precisely why the American models refused.

So in the case of a major coding/hack related nightmare, you have no choice but to use Chinese models to investigate the issue because they are less nerfed than the American versions. Claude and OAI both knew the answer to this weakness and refused to help. If you are a developer running code, under pressure because something has gone wrong or you have identified a weakness, you are stuck. Only the open-source Chinese models can help you unless you are some sort of specifically approved American company.

What good will come from this? Well, hardware wallet security is going to get a lot better and it will have to. Everyone is throwing unlimited tokens at their security code, and doing so almost exclusively with the Chinese models. I suspect a lot of things have quietly been hacked over the last few months and we will read about them only over the next few years.

Some people have questioned ColdCard for years. Mostly because if you challenged them on their software you would be instantly attacked on social media.

He is clearly now having his moment of smug satisfaction. No comfort there for those affected by the issue, which it must be said was a 101 error. Insufficient entropy from a hardware wallet.

Red Team

The whole event has produced a red team effort across the ecosystem. In hacking terms 'red team' means the good guys simulating attacks on systems to test them. As you can see, it is almost entirely a Chinese model effort.

Note the suggestion that most people "truly have no idea what is about to happen". I do believe a lot of things have been hacked in the last few months, probably a lot of major corporations, websites, banks, you name it. Defences have been breached and all is calm (except at ColdCard) but the next six months will tell us. Worth noting too that the very best hacks just stay unknown. When Google got hacked years ago, the hackers sat in the system for years without anyone knowing.

Is it scary? Yes it is because only the most battle hardened systems are going to survive this.

They've been good to us

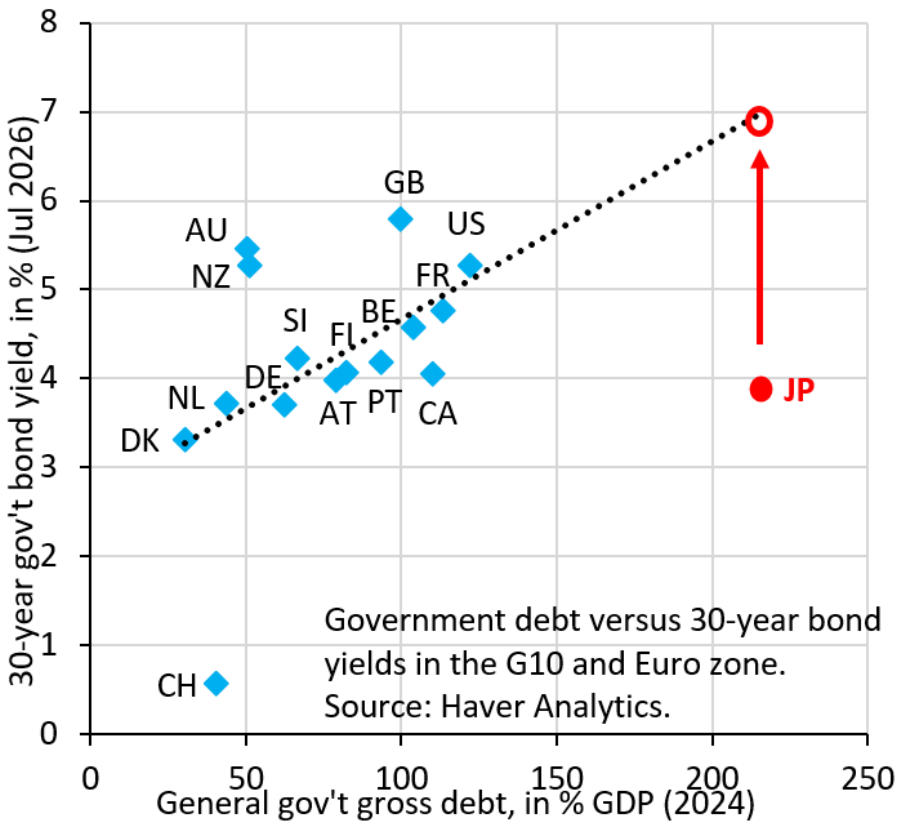
On why America is intervening in the Japanese foreign exchange market:

"...they've been good to us, apart from Pearl Harbor"

Trumpian diplomacy at its finest this week. The real reason of course is that if America doesn't help, then Japan will dump its US bond holdings and use the money to prop up the yen. Otherwise currency collapse would precipitate inflation, interest rates would go up sharply….the end. It's a nightmare scenario.

For the US, the bond dumping would be extremely unhelpful since they have rather a lot of bonds to unload themselves. Mutually helpful then if the US just buys bucket loads of yen.

I find this chart instructive on the matter, mapping the scale of debt to the interest rate. Fairly clear line and some unpopular outliers, GB and AU in particular. That's because the market believes they will move along the x axis of gross government debt relatively more quickly than other countries. It's a political judgement on the British and Australian governments and the bond market takes no prisoners.



On the other side of the coin is Japan. At its debt level of 220% of GDP, the interest rate 'ought to be' 7% and it's nowhere near. 7% would be the end, within 20 years the entire government budget would be consumed by interest payments. Obviously the bond market would sniff that collapse a long way out, so it wouldn't take anywhere near that long.

Difficult problem. Japan, joining Australia as the 51st and 52nd US states in all but name. Whisper it though, people get very upset.

UBI

Government contracts to require job creation instead of green targets under new rules

Louise Haigh says taxpayer money must benefit local communities amid backlash from environmental groups

Back in 2021 we covered a Universal Basic Income experiment run by the Welsh government. It was the stupidest of stupidities and promptly failed because it just gave people money and required nothing in return. You might call it pure UBI. That strategy fails because it antagonises people that are not getting the free money, generally they are in the majority.

Still, I remain a believer that not only is UBI coming, it is here. It also explains the near total collapse in productivity growth in some countries, including Australia.

In the UK, the most recent iteration of UBI came from the new First Secretary of State, Louise Haigh. It requires that to secure government contracts you need to demonstrate that you are going to create jobs. It replaces the previous requirement that you build a windmill nobody asked for.

Central government departments are required to weigh up the social value of government contracts, which counts for 10% of the decision. Under new measures this will be increased to 20%, but instead of considering social good, government buyers will be pushed to secure contracts with companies creating local jobs that pay above the minimum wage, offer training, work experience or plug local skills gaps.

It's fairly simple then. Assume I tender for a government contract for £5m and include that I will employ two people and complete the task in ten days. I compete against someone who tenders and says I will use only machines and robots and no humans. It will be complete in seven days. Who wins this contract? If you are a bureaucrat working for a politician that wants more jobs, what choice do you have? *"Hi Minister, we saved three days"*. I think not.

A false example of course but the policy runs entirely against the grain of productivity. In the private sector, when you have to use *your own money* the question is almost entirely "how can I do this at the lowest possible cost with the fewest possible people? Can we buy a machine that can do it? Can we program it?"

This is still universal basic income though. People are getting slightly overpaid to work slightly more slowly and yes it might be good for them, but bad for everyone else. Just like in Wales.

Back then to the architect of the scheme. The new First Secretary is interesting because she is one of the few government ministers to have had a job in the private sector. She worked for Aviva, a large insurance company. She left that job after she was convicted of fraud for falsely claiming her mobile phone had been stolen so she could upgrade to an iPhone 5. She was given the lowest possible sentence, a conditional discharge.

She is now the second highest ranking government minister. First Secretary of State, Chancellor of the Duchy of Lancaster and Minister for the Cabinet Office. It's not really the fraud conviction itself, there are Members of Parliament who have done far, far worse, some in very recent memory. A nothingburger really, it was just a terrible decision and a terrible judgement.

That's the issue though, the person running the joint just has terrible judgement. The new policy is a bit like the phone decision. Sounds like a good idea, 'doesn't hurt anyone' but is just monumentally stupid.

Euro-Trash

Time flies. It seems like only last year we were on the last round of European banknotes. Once again the ECB is running a competition for designs and the finalists are here. It would appear you do not need to be European to vote either, naturally I have participated. Some of them are frankly weird too.

The general public, as usual, did a far better job. My personal favourite is the memorial to the Nord Stream pipeline which you will all remember the "Russians" blew up. Immediately after which we never heard about it again.


© BCE ECB EZB EKT EKP
1000
TRILLION
1000 EURO
TRILLION


© BCE ECB EZB EKT EKP 1984
Big Brother
50
1984
BIG BROTHER
IS WATCHING
YOU
50 EURO
EYPΩ


© ECB EUR·SISTEMS ECB EC·00·B
50
EUROS
EUPOS
EBPOP
50


ACAB
EUROENLS EUROCTA B2 EPRO EVTSE TI8 SN
5
EURO
EYPO
EYPO


EUROPEAN CENTRAL BANK
ONE HUNDRED EURO
BB 987654321
EUROPEAN UNION
100 EURO
AA 123456789
CLEON PETERSON
100


BCE ECB EZB EKT EKP 2024
M. Draghi
100
EUREAN UNION ΕΥΡΩΡΕΑΪΚΗ ΕΝΩΣΗ ΕΝΩΣΗ ΕΥΡΩΠΗ EUROPENE ΕΙΘΣ
100 EURO
ΕΥΡΩ
ΕΒΡΟ
100